



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,424	08/30/2000	Mariusz H. Jakubowski	MS1-528US	2561
22801 7590 03/26/2007 LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			EXAMINER TRAN, TONGOC	
			ART UNIT 2134	PAPER NUMBER

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/26/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/26/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on December 29, 2006. Claims 1, 3-4, 8-9, 11-12, 25 and 31 have been amended. Claim 1-9, 11-16, 25-31 and 33-36 are pending.

Response to Arguments

2. Applicant's arguments, with respect to the amended claims have been fully considered and are persuasive. Claims 1-9, 11-16 and 31 previously rejected under 35 U.S.C. 103 have been withdrawn. With respect to claims 25-30, Applicant contends that the cited prior art fail to teach or suggest "an analyzer to parse the original digital good along natural boundaries into segments; the production server being configured to identify a first segment in the original digital good and use a byte or bit values from the first segment in an S-box when encrypting a second segment of the original digital good" as recited in claim 25. Examiner respectfully disagrees. Alrabady and Graunke teach segmenting data into first and second portion and using one portion as key or S-box to encrypt or decrypt another portion. Since a parser is inherently required in order to segment data at a predetermined boundaries and substituting portion of data as key to encrypt the other portion encompasses parsing data and taking a segment of data as key (in byte or bits size) to encrypt the other portion of the data. Therefore, the limitation is met. With respect to claims 33-36, because Applicant fails to amend the claims or to address the claim rejection, the rejection has been maintained.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 25-30 and 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alrabady et al. (U.S. Patent No. 6,829,357) in view of Graunke (U.S. Patent No. 6,804,355).

In respect to claim 33, Alrabady discloses a computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

Selecting a portion of a digital good; selecting another portion of the digital good, wherein the other portion is to be decrypted; and using the portion as a key when encrypting the other portion (see col. 1, line 65-col. 2, line 5 and col. 3, line 60-col. 4, line 15). Alrabady does not specifically disclose but Graunke discloses using a key as a substitution box in encryption and decryption (S-box) (see col. 2, lines 53-56). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a key as S-box taught by Graunke with using one portion of message as a key to encrypt and decrypt another portion of message taught by Alrabady for the advantage of the resistance to differential and linear cryptanalysis that S-boxes brings.

Art Unit: 2134

In respect to claims 30 and 34, Alrabady and Graunke further disclose wherein the encryption process uses a Data Encryption Standard (DES) cipher (see Graunke, col. 1, lines 18-20).

In respect to claims 27 and 35, Alrabady and Graunke further disclose wherein the using comprises using bits of the portion to determine a substitution sub-portion for each sub-portion in the other portion (see Graunke, col. 5, lines 25-49).

In respect to claims 29 and 36, Alrabady and Graunke further disclose wherein the digital good comprises a software program and video content (see Alrabady, col. 4, lines 1-2).

In respect to claim 25, Alrabady discloses a production system comprising:

A memory to store an original digital good, wherein the original digital good is transformed into a protected digital good; an analyzer to parse the original digital good along natural boundaries into segments (parser is inherently required in order to segment data at a predetermined boundaries); and

A production server equipment with a substitution box (S-box) protection tool that is used to augment the original digital good for protection purposes, the production server being configured to identify a first segment in the original digital good and use a byte or bit values from the first segment in an S-box when encrypting a second segment of the original digital good (see col. 1, line 65-col. 2, line 5 and col. 3, line 60-col. 4, line

Art Unit: 2134

15). Alrabady does not specifically disclose but Graunke discloses using a key as a substitution box in encryption and decryption (S-box) (see col. 2, lines 53-56). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement a key as S-box taught by Graunke with using one portion of message as a key to encrypt and decrypt another portion of message taught by Alrabady for the advantage of the resistance to differential and linear cryptanalysis that S-boxes brings.

In respect to claim 28, Alrabady and Graunke further disclose the server configured to use the first segment as an S-box by determining for each group of bits of the second segment, a new group of bits based on the first segment (see Alrabady, col. 4, lines 16-46).

Allowable Subject Matter

4. Claims 1-9 and 11-16 are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2134

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 17, 2007


KAMBIZ ZAND
PRIMARY EXAMINER